WHAT IS CLAIMED IS:

1. An unauthorized access detection device for detecting unauthorized accesses over a network, comprising:

unauthorized access scenario storage means for storing unauthorized access scenarios each defining a procedure of processes to be executed over the network until an unauthorized access is made through preparation;

ongoing scenario storage means for storing ongoing scenarios by relating the ongoing scenarios to key data, the ongoing scenarios each indicating progress of processes executed over the network based on one of the unauthorized access scenarios, the key data differentiating processes associated with each of the ongoing scenarios from other processes;

key data extraction means for obtaining a packet traveling on the network and extracting the key data from the packet obtained;

ongoing scenario detection means for retrieving an ongoing scenario from the ongoing scenario storage means with the key data extracted by the key data extraction means as a search key;

check means for determining whether execution of a process indicated by the packet after the ongoing scenario retrieved by the ongoing scenario detection means follows one of the unauthorized access scenarios being stored in

the unauthorized access scenario storage means;

ongoing scenario update means for updating the ongoing scenario being stored in the ongoing scenario storage means when a check result of the check means shows that the execution follows the one of the unauthorized access scenarios; and

report output means for outputting an unauthorized access report showing progress of processes executed based on the one of the unauthorized access scenarios, depending on the check result of the check means.

2. The unauthorized access detection device according to claim 1, wherein the report output means outputs the unauthorized access report when the ongoing scenario retrieved by the ongoing scenario detection means reaches a final stage of the one of the unauthorized access scenarios.

3. The unauthorized access detection device according to claim 1, wherein:

the ongoing scenario storage means stores a numeric value by relating the numeric value to the each of the ongoing scenarios, the numeric value indicating a degree of progress of the each of the ongoing scenarios; and

the ongoing scenario update means updates the ongoing scenario by increasing the numeric value of the degree of progress.

4. The unauthorized access detection device according to claim 3, wherein the report output means outputs the unauthorized access report when the degree of progress exceeds a prescribed value.

5. The unauthorized access detection device according to claim 1, wherein:

in the unauthorized access scenario storage means, roles are set to a source and a destination of information indicating a process to be executed over the network, in each of the unauthorized access scenarios; and

the check means determines whether a source and a destination of the process indicated by the packet take the roles defined in the one of the unauthorized access scenarios.

6. The unauthorized access detection device according to claim 1, wherein:

a procedure of processes until an unauthorized access is made through preparation is defined in the form of state transitions with events as turning points in each of the unauthorized access scenarios being stored in the unauthorized access scenario storage means, the events generated at a time of instructions and responses of processes executed over the network; and

the check means determines whether a state

transition to an event of the process indicated by the packet follows the one of the unauthorized access scenarios.

7. The unauthorized access detection device according to claim 1, wherein:

valid periods for proceeding processes to next stages are set in each of the unauthorized access scenarios being stored in the unauthorized access scenario storage means; and

the check means determines whether the process indicated by the packet is executed within the valid period.

8. The unauthorized access detection device according to claim 1, wherein:

weights to be added every time when a scenario progresses are defined in each of the unauthorized access scenarios being stored in the unauthorized access scenario storage means; and

the report output means outputs the unauthorized access report when a total weight exceeds a prescribed value.

9. An unauthorized access detection method for detecting unauthorized accesses over a network, comprising the steps of:

obtaining a packet traveling on the network and extracting prescribed key data from the packet obtained;

retrieving an ongoing scenario from ongoing scenario storage means with the key data extracted from the packet as a search key, the ongoing scenario indicating progress of processes executed over the network based on an unauthorized access scenario, the unauthorized access scenario defining a procedure of processes to be executed over the network until an unauthorized access is made through preparation, the key data differentiating processes associated with the ongoing scenario from other processes;

checking unauthorized access scenario storage means storing the unauthorized access scenario to determine whether execution of a process indicated by the packet after the ongoing scenario retrieved follows the unauthorized access scenario;

updating the ongoing scenario being stored in the ongoing scenario storage mans when a check result shows that the execution follows the unauthorized access scenario; and

outputting an unauthorized access report indicating progress of processes executed based on the unauthorized access scenario, depending on the check result.

10. An unauthorized access detection program to detect unauthorized accesses over a network, the

unauthorized access detection program causing a computer to function as:

unauthorized access scenario storage means for storing unauthorized access scenarios each defining a procedure of processes to be executed over the network until an unauthorized access is made through preparations;

ongoing scenario storage means for storing ongoing scenarios by relating the ongoing scenarios to key data, the ongoing scenarios each indicating progress of processes executed over the network based on one of the unauthorized access scenarios, the key data differentiating processes associated with each of the ongoing scenarios from other processes;

key data extraction means for obtaining a packet traveling on the network and extracting the key data from the packet obtained;

ongoing scenario detection means for retrieving an ongoing scenario from the ongoing scenario storage means with the key data extracted by the key data extraction means as a search key;

check means for determining whether execution of a process indicated by the packet after the ongoing scenario retrieved by the ongoing scenario detection means follows one of the unauthorized access scenarios being stored in the unauthorized access scenario storage means;

ongoing scenario update means for updating the ongoing scenario being stored in the ongoing scenario

storage means when a check result of the check means shows that the execution follows the one of the unauthorized access scenarios; and

report output means for outputting an unauthorized access report showing progress of processes executed based on the one of the unauthorized access scenarios, depending on the check result of the check means.

11. A computer-readable recording medium storing an unauthorized access detection program to detect unauthorized accesses over a network, the unauthorized access detection program causing a computer to function as:

unauthorized access scenario storage means for storing unauthorized access scenarios each defining a procedure of processes to be executed over the network until an unauthorized access is made through preparation;

ongoing scenario storage means for storing ongoing scenarios by relating the ongoing scenarios to key data, the ongoing scenarios each indicating progress of processes executed over the network based on one of the unauthorized access scenarios, the key data differentiating processes associated with each of the ongoing scenarios from other processes;

key data extraction means for obtaining a packet traveling on the network and extracting the key data from the packet obtained;

ongoing scenario detection means for retrieving an ongoing scenario from the ongoing scenario storage means with the key data extracted by the key data extraction means as a search key;

check means for determining whether execution of a process indicated by the packet after the ongoing scenario retrieved by the ongoing scenario detection means follows one of the unauthorized access scenarios being stored in the unauthorized access scenario storage means;

ongoing scenario update means for updating the ongoing scenario being stored in the ongoing scenario storage means when a check result of the check means shows that the execution follows the one of the unauthorized access scenarios; and

report output means for outputting an unauthorized access report showing progress of processes executed based on the one of the unauthorized access scenarios, depending on the check result of the check means.